UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/756,744	01/13/2004	Morton D Swimmer	CH920020012US1	1837

7590 04/21/2008

IBM CORPORATION
Anne Vachon Dougherty, Esq.
3173 Cedar Road
Yorktown Heights, NY 10598

EXAMINER	
ALMEIDA, DEVIN E	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
04/21/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/756,744	Applicant(s) SWIMMER ET AL.	
	Examiner DEVIN ALMEIDA	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 January 2008*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4,5,12-16,19 and 20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4,5,12-16,19 and 20* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

This action is in response to the papers filed 9/10/2007. Claims 1, and 15-19, Currently claims 1-19 are under consideration.

Response to Arguments

Applicant's arguments have been fully considered but they are moot in view of new grounds of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 2, 15 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Van Der Made (U.S. Patent 7,093,239) in view of Kilpatrick et al (U.S. 6,735,703) in view of Kolichtchak (U.S. 2003/0014667).

Van Der Made teaches with respect to claims 1, 15, and 16, a method for preventing attacks in a monitored data processing system comprising the steps of:

detecting an intrusion into the data processing system (see Van Der Made abstract); monitoring from a daemon executed in a memory of the monitored data processing system (see Van Der Made column 2 lines 50 – column 3 line 15); upon detection of an intrusion, identifying a malicious code string related to the detected intrusion (see Van Der Made abstract) by matching the system calls with one or more of established patterns and rules contained in a pattern matcher and representing a model of normal behavior (see Van Der Made abstract), wherein the matching of the system calls comprises establishing a non-deterministic automaton based on an analysis of executable code of the daemon (see Van Der Made column 2 lines 50 – column 3 line 15); extracting the malicious code string by the step of: intercepting the system call via a subprogram of the sensor for observing the interaction of the daemon and the operating system (see Van Der Made abstract and column 2 line 50 – column 3 line 15); and forwarding the malicious code string to an intrusion limitation subsystem to reduce further intrusions based on the malicious code string (see Van Der Made abstract i.e. store patterns and sequences with there corresponding analysis results).

Van Der Made does not teach detecting an intrusion into the data processing system by monitoring system calls; inspecting a stack upon detection of an intrusion to retrieve an address leading to the malicious code string; locating, as a first element on the stack, a return address of a system call entry code from which the subprogram departed; retrieving a return address of the malicious code string pointing to a memory location in the range in which the daemon is executed from a second element on the stack positioned at or near the location of the return address of the system call entry code to facilitate finding and extracting of the malicious code string; scanning the memory range owned by the executed daemon starting from the return address in opposite directions until on one side a first region with a plurality of similar addresses and on the other side a second region with a plurality of similar instructions that do not alter the sequential control flow is identified (see Kolichtchak paragraph 0032); extracting the malicious code string from between the first and second regions (see Kolichtchak paragraph 0032).

Kilpatrick teaches detecting an intrusion into the data processing system by monitoring system calls (see Kilpatrick column 2 lines 11-22). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have monitoring system calls to determine whether the system calls of a monitored process conform to the profiles of expected behavior (see Kilpatrick column 2 lines 11-22). Therefore one would have been motivated to have monitoring system calls.

Kolichtchak teaches the steps of inspecting a stack upon detection of an intrusion to retrieve an address leading to the malicious code string (see Kolichtchak paragraph 0032); locating, as a first element on the stack, a return address of a system call entry code from which the subprogram departed (see Kolichtchak paragraph 0032); and retrieving a return address of the malicious code string pointing to a memory location in the range in which the daemon is executed from a second element on the stack positioned at or near the location of the return address of the system call entry code to facilitate finding and extracting of the malicious code string (see Kolichtchak paragraph 0032); scanning the memory range owned by the executed daemon starting from the return address in opposite directions until on one side a first region with a plurality of similar addresses and on the other side a second region with a plurality of similar instructions that do not alter the sequential control flow is identified (see Kolichtchak paragraph 0032); and extracting the malicious code string from between the first and second regions (see Kolichtchak paragraph 0032). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have inspected the stack upon detection of an intrusion to retrieve an address leading to the malicious code string to stop the spread of the malicious code and the effects of buffer overflow attacks (see Kolichtchak paragraph 0001-0004). Therefore one would have been motivated to have inspected the stack upon detection of an intrusion to retrieve an address leading to the malicious code string.

With respect to claim 2, wherein the intrusion limitation subsystem comprises a pattern filter in the monitored system, and wherein said pattern filter compares incoming strings to the malicious code string for reducing further intrusions based on the malicious code string (see Van Der Made abstract i.e. store patterns and sequences with there corresponding analysis results).

Claims 4, 5 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hoefelmeyer et al (U.S. Patent 7,043,757) in view of Kephart et al (U.S. Patent # 6,016,546).

Hoefelmeyer teaches with respect to claims 12, a method for preventing attacks in a monitored data processing system comprising the steps of: detecting an intrusion into the data processing system (see Hoefelmeyer column 6 lines 25-35); upon detection of an intrusion, identifying a malicious code string related to the detected intrusion (see Hoefelmeyer column 6 lines 25-35 i.e. viruses are detected by the detection manager system); extracting the malicious code string (see column 6 lines 25-35); extracting the malicious code string (see Hoefelmeyer column 6 lines 25-35); storing each malicious code string extracted in a database of the response server (see Hoefelmeyer column 6 lines 25-43); forwarding the malicious code string to an intrusion limitation subsystem to reduce further intrusions based on the malicious code string (see Hoefelmeyer column 6 lines 25-43 i.e. upon detection of a new virus the detection manager system transmits the new signature to the remote site scanning system), wherein the intrusion limitation subsystem comprises a response server (see Hoefelmeyer column 6 lines 25-35 i.e. detection manager system) and wherein said response server distributes the malicious code string to one or more connected systems (see Hoefelmeyer column 6 lines 25-35 i.e. detection manager system transmits the new signatures to the remote site scanning system) to reduce further intrusions into such connected systems based on the malicious code string (see Hoefelmeyer column 6 lines 25-35)

Hoefelmeyer does not teach correlating the stored malicious code strings to find sets of malicious code; and for each set, generating a signature that allows the individual identification of all malicious code strings contained in the corresponding set.

Kephart teaches correlating the stored malicious code strings to find sets of malicious code strings (see Kephart column 6 line 49 – column 7 line 28); and for each set, generating a signature that allows the individual identification of all malicious code strings contained in the corresponding set (see Kephart column 6 line 49 – column 7 line 28). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have grouped similar malicious code strings together to help reduce the amount of memory required to scan a given data string for the presence of computer viruses (see Kephart column 1 lines 56-65). Therefore one would have been motivated to have grouped similar malicious code strings together.

With respect to claim 4, wherein the one or more connected systems comprise one or more connected monitored systems (see Hoefelmeyer figure 2).

With respect to claim 5, wherein the one or more connected systems comprise one or more connected monitoring systems (see Hoefelmeyer figure 2).

Claims 13, 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hoefelmeyer et al (U.S. Patent 7,043,757) in view of Kephart et al (U.S. Patent # 6,016,546) in further view of Lamburt et al (U.S. Patent # 6,374,241). Hoefelmeyer, and Kephart teach everything with respect to claim 12 above but with respect to claim 13 they do not teach wherein the correlating comprises utilizing an edit-distance algorithm. Lamburt teaches wherein the correlating comprises utilizing an edit-distance algorithm (see Lamburt column 41 lines 4-62). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have used a edit-distance algorithm to how far apart two strings of data are. Therefore one would have been motivated to have grouped similar malicious code strings together using a edit-distance algorithm and group them based on a distance smaller than a given distance apart (see Lamburt column 41 lines 4-62).

With respect to claim 14, wherein the sets have mutual edit distances smaller than a given threshold distance (see Lamburt column 41 lines 4-62).

Claims 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Van Der Made (U.S. Patent 7,093,239) in view of Kilpatrick et al (U.S. 6,735,703) in view of Kolichtchak (U.S. 2003/0014667) in further view of Hoefelmeyer et al (U.S. Patent 7,043,757) in view of Lamburt et al (U.S. Patent # 6,374,241).

Van Der Made, Kilpatrick and Kolichtchak teach everything with respect to claim 15 and 15 above but they do not teach with respect to claim 19 wherein the intrusion limitation subsystem comprises a response server comprising: a database for receiving extracted malicious code strings from the code extractor; a correlate connected to the database for assembling sets of code strings having mutual edit distances less than a given threshold distance; a sequencer connected to the database for generating signatures, wherein a signature is generated for each set to facilitate identification of all malicious code strings contained in the corresponding set; and a distributor connected to the database for distributing signatures to connected systems.

Hoefelmeyer teaches wherein the intrusion limitation subsystem comprises a response server comprising: a database for receiving extracted malicious code strings from the code extractor (see Hoefelmeyer column 6 lines 25-43) and a distributor connected to the database for distributing signatures to connected systems (see

Hoefelmeyer figure 2 and column 6 lines 25-43). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have a sent new signatures of virus to a remote site to allow other computers on the network to also be updated with the new virus signature. Therefore one would have been motivated to have sent new signatures of virus to a remote site (see Hoefelmeyer column 6 lines 25-43).

Lamburt theaches a correlate connected to the database for assembling sets of code strings having mutual edit distances less than a given threshold distance (see Lamburt column 41 lines 4-62); a sequencer connected to the database for generating signatures, wherein a signature is generated for each set to facilitate identification of all malicious code strings contained in the corresponding set (see Lamburt column 41 lines 4-62). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have used a edit-distance algorithm to how far apart two strings of data are. Therefore one would have been motivated to have grouped similar malicious code strings together using a edit-distance algorithm and group them based on a distance smaller than a given distance apart (see Lamburt column 41 lines 4-62).

With respect to claim 20, storing each malicious code string extracted in a database of the response server (see Hoefelmeyer column 6 lines 25-43); correlating the stored malicious code strings to find sets of malicious code strings (see Lamburt column 41 lines 4-62); and for each set, generating a signature that allows the individual identification of all malicious code strings contained in the corresponding set (see

Lamburt column 41 lines 4-62); and forwarding the malicious code string to an intrusion limitation subsystem to reduce further intrusions based on the malicious code string wherein the intrusion limitation subsystem comprises a response server and wherein said response server distributes the malicious code string to one or more connected systems to reduce further intrusions into such connected systems based on the malicious code string (see Hoefelmeyer figure 2 and column 6 lines 25-43).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Devin Almeida whose telephone number is 571-270-1018. The examiner can normally be reached on Monday-Thursday from 7:30 A.M. to 5:00 P.M. The examiner can also be reached on alternate Fridays from 7:30 A.M. to 4:00 P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Devin Almeida
Patent Examiner
4/16/2008

/Benjamin E Lanier/
Primary Examiner, Art Unit 2132